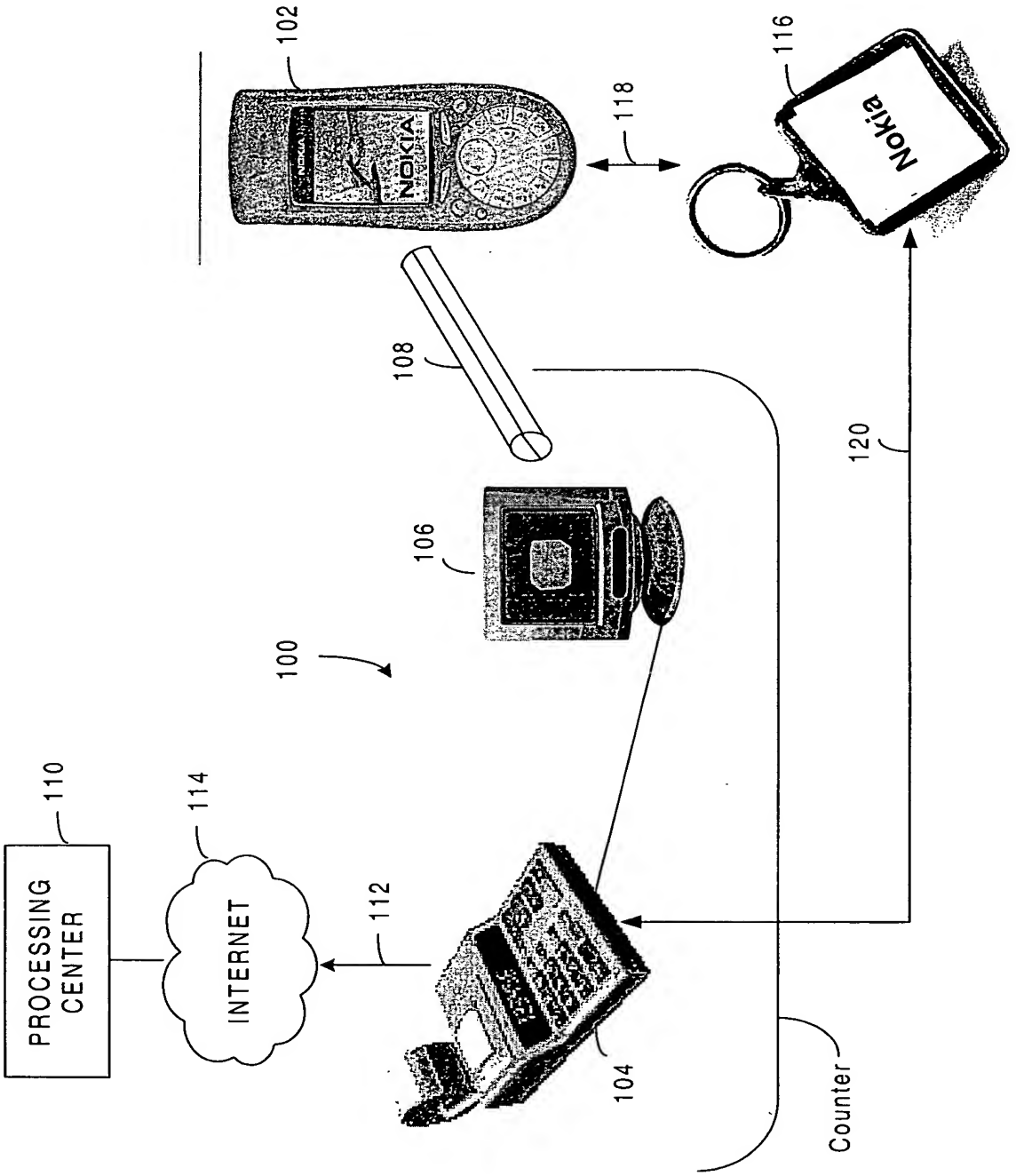

102
NOKIA
118
116
Nokia
108
120
106
100
PROCESSING CENTER
110
INTERNET
114
112
104
Counter

Fig. 1

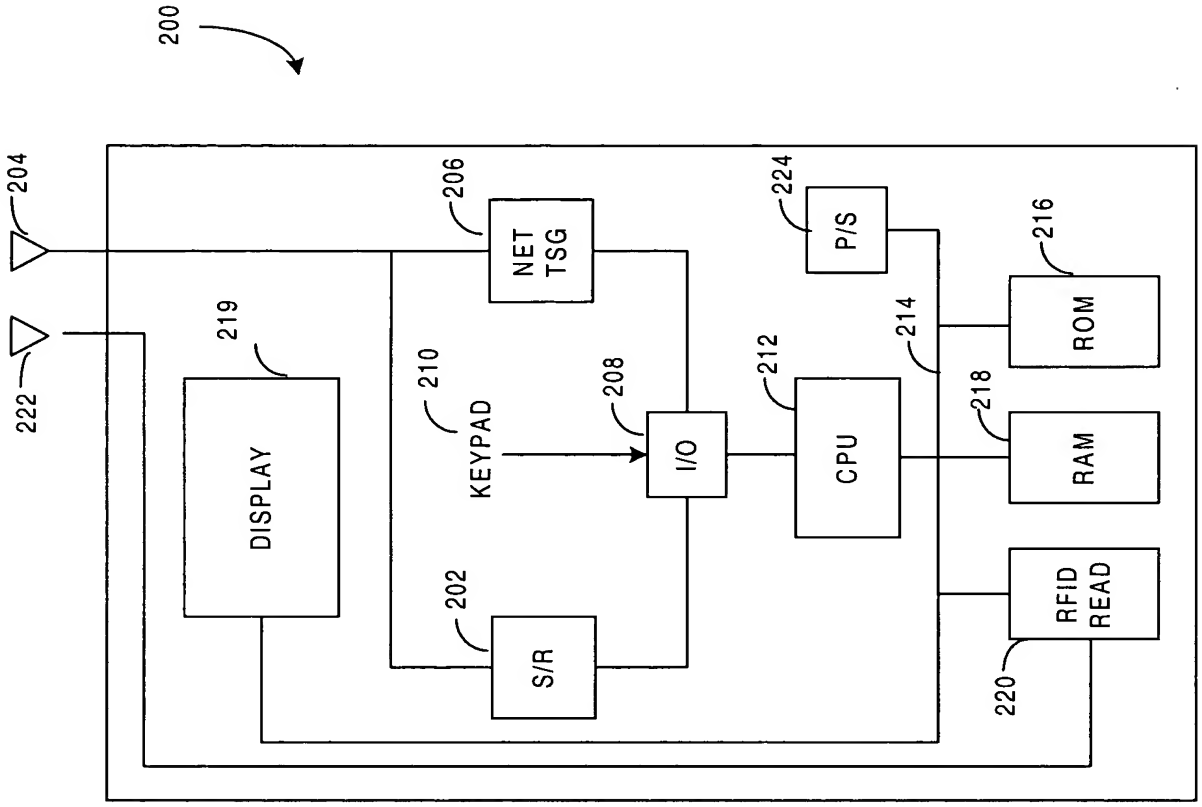

200
204
222
206
NET TSG
224
P/S
216
ROM
219
DISPLAY
210
KEYPAD
208
I/O
212
CPU
214
218
RAM
202
S/R
RFID READ
220

Fig. 2

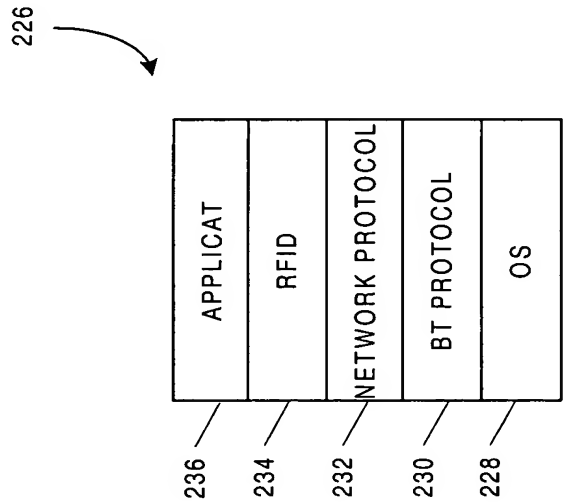

226
APPLICAT
RFID
NETWORK PROTOCOL
BT PROTOCOL
OS
236
234
232
230
228

Fig. 2A

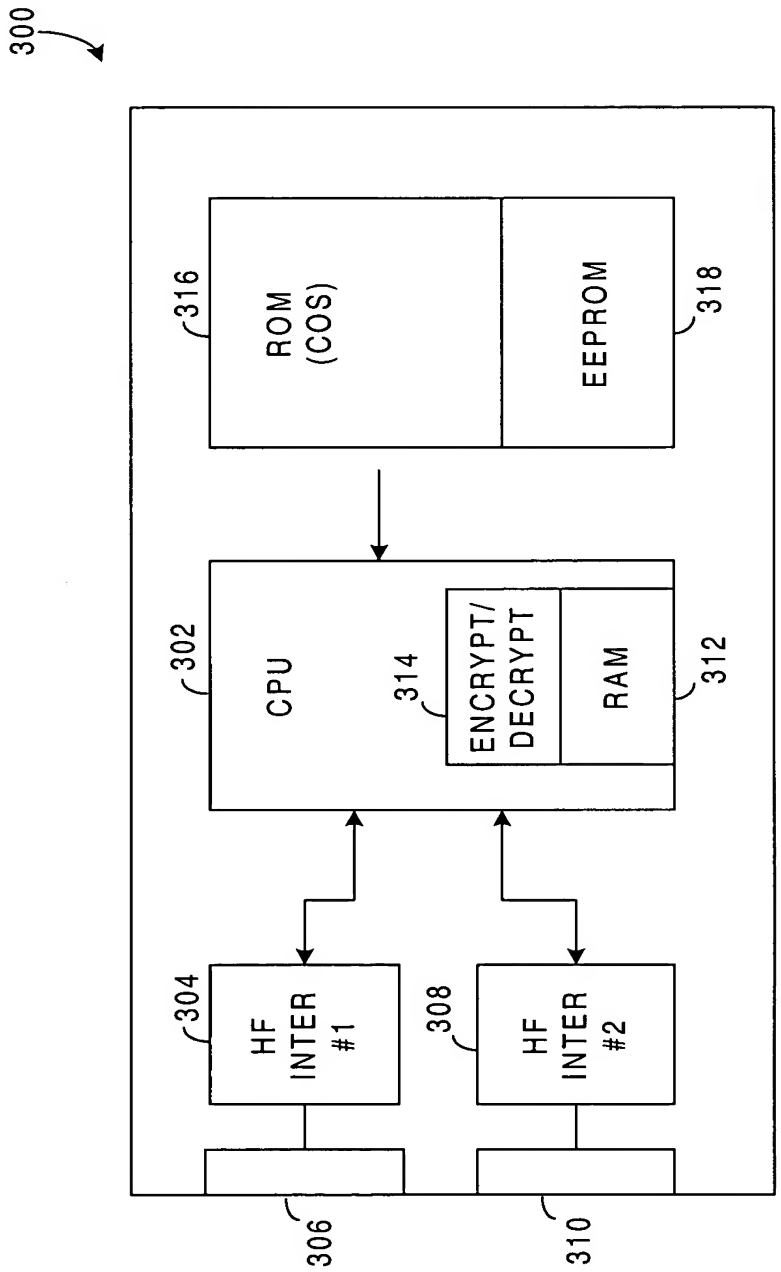

300
316
ROM (COS)
EEPROM
318
302
CPU
314
ENCRYPT/ DECRYPT
RAM
312
304
HF INTER #1
308
HF INTER #2
306
310

Fig. 3

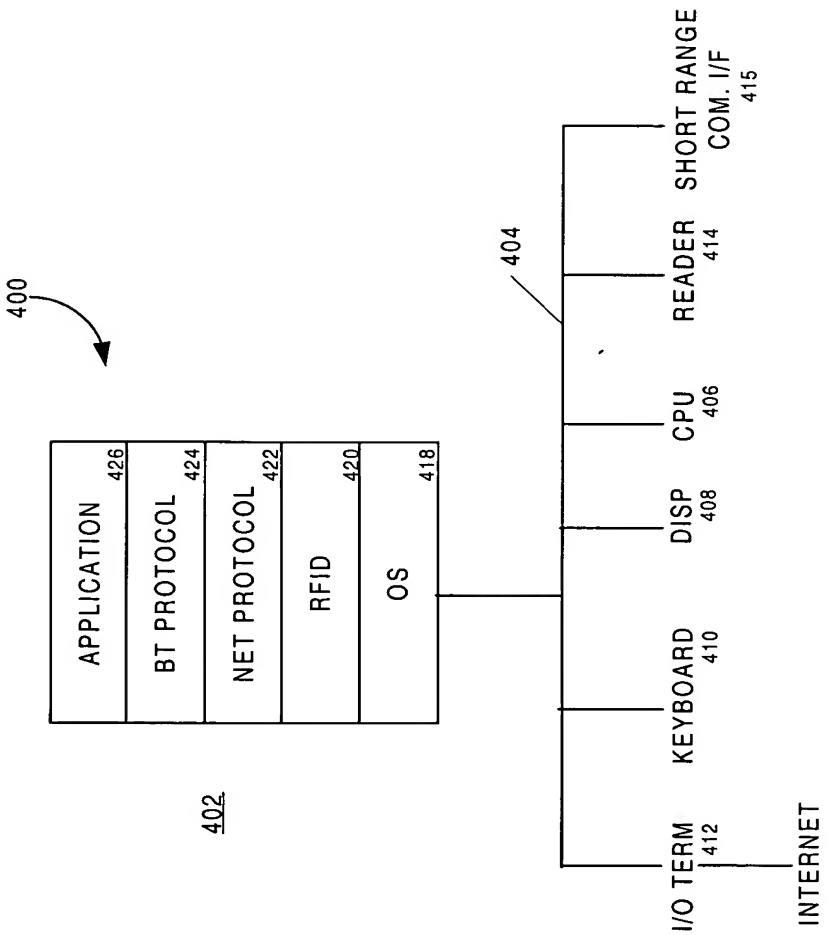

400
APPLICATION
426
BT PROTOCOL
424
NET PROTOCOL
422
RFID
420
OS
418
402
404
SHORT RANGE COM. I/F
415
READER
414
CPU
406
DISP
408
KEYBOARD
410
I/O TERM
412
INTERNET

Fig. 4

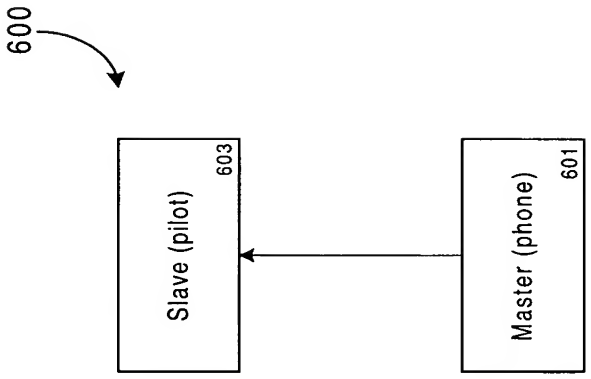
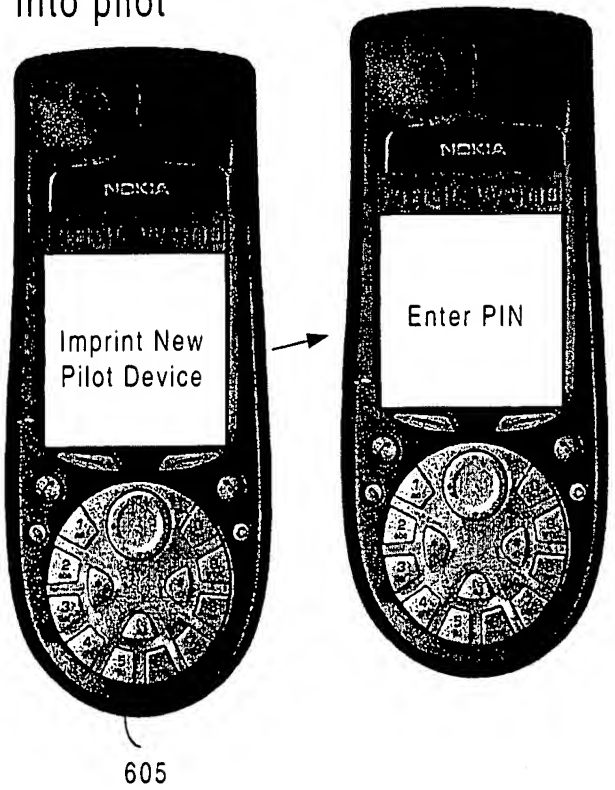
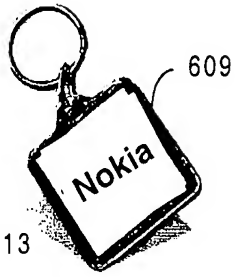


Fig. 5

User launch MW application for writing authorization information into pilot



If imprinting was successful, then MAC address and K will be stored into smar card



Imprinting Hello 607

PIN request, RAND 611

RES, MAC address, Secret K 613

Imprinting done/failed 615

Here RES is result computed from PIN and Challenge RAND

Fig. 5A

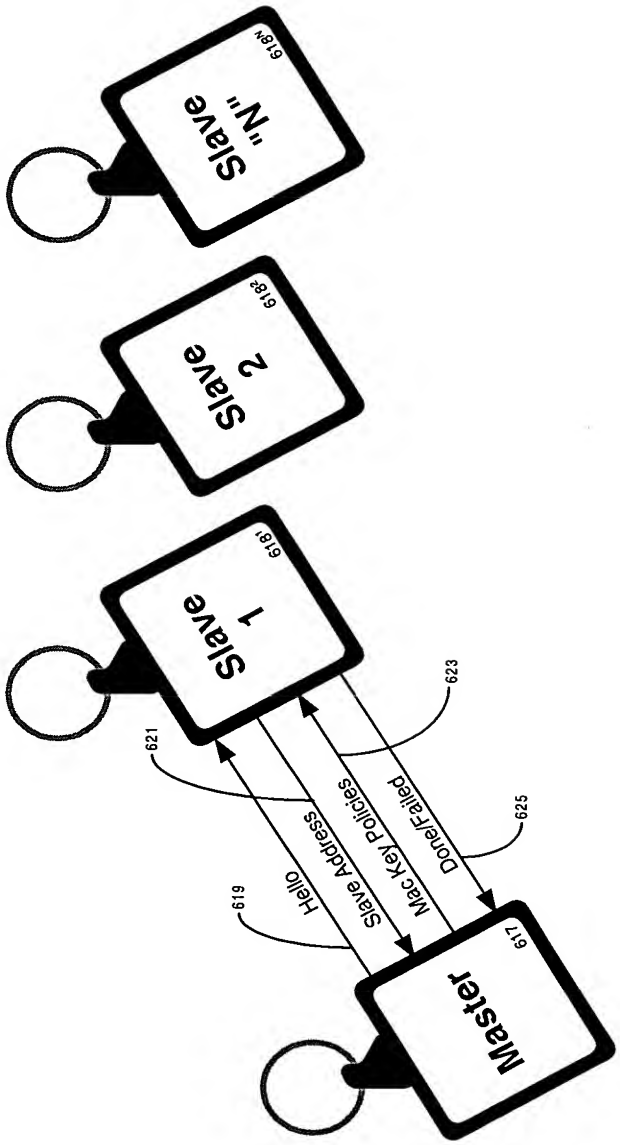

Slave "N"
618N
Slave 2
6182
Slave 1
6181
Master
617
Hello
619
Slave Address
Mac Key Policies
Done/Failed
621
623
625

Fig 5B

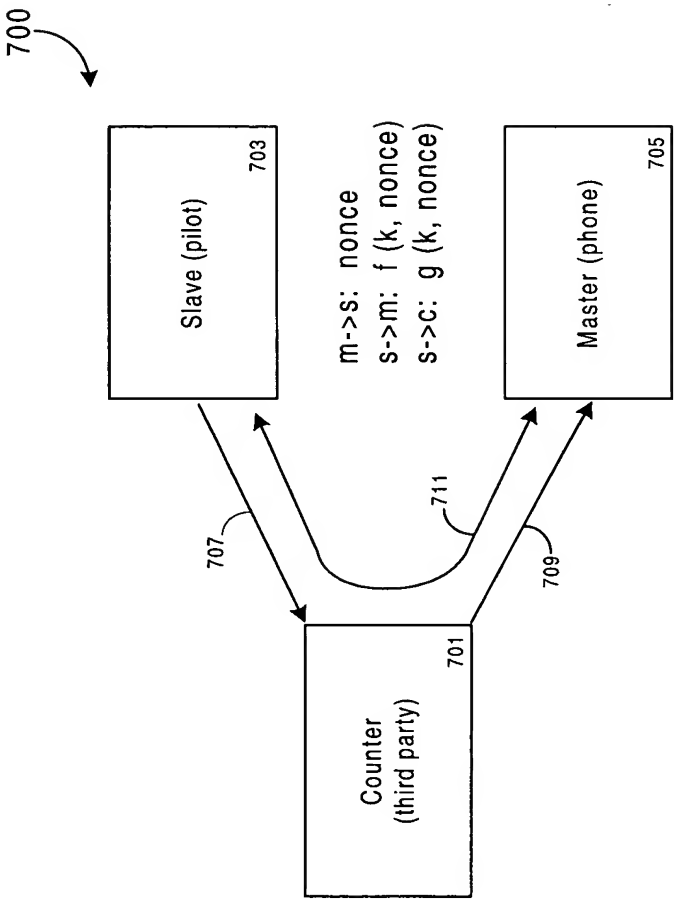

700
Slave (pilot)
703
m->s: nonce
s->m: f (k, nonce)
s->c: g (k, nonce)
Master (phone)
705
707
711
709
Counter
(third party)
701

FIG. 6

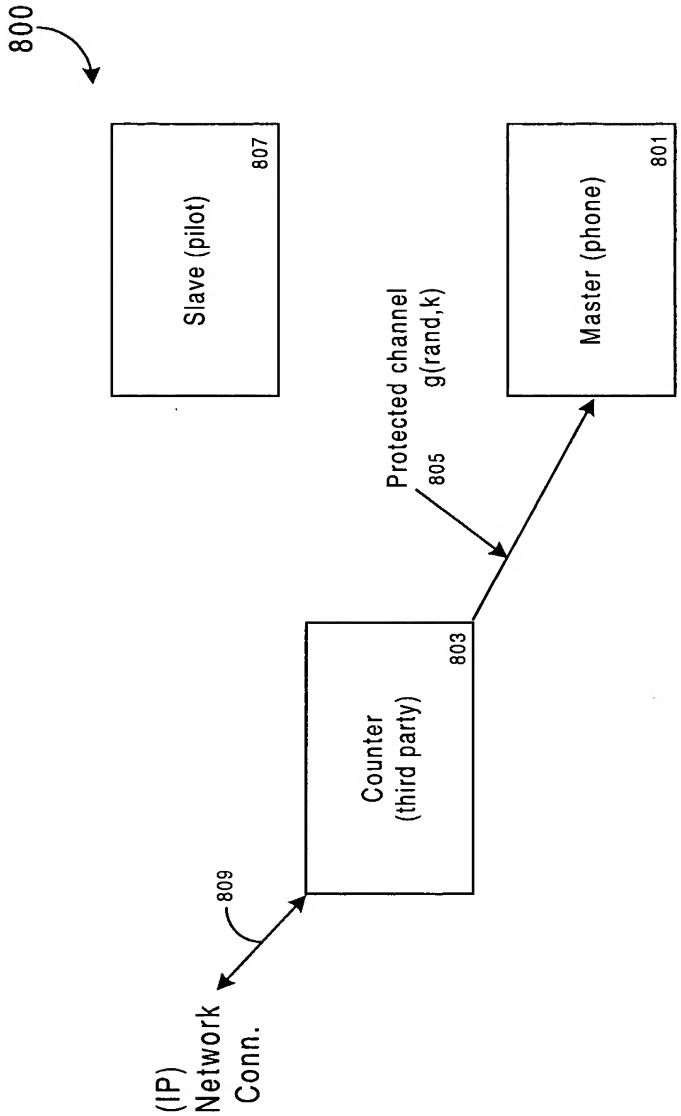

800
Slave (pilot)
807
Master (phone)
801
Protected channel
g(rand,k)
805
Counter
(third party)
803
809
(IP)
Network
Conn.

FIG. 7

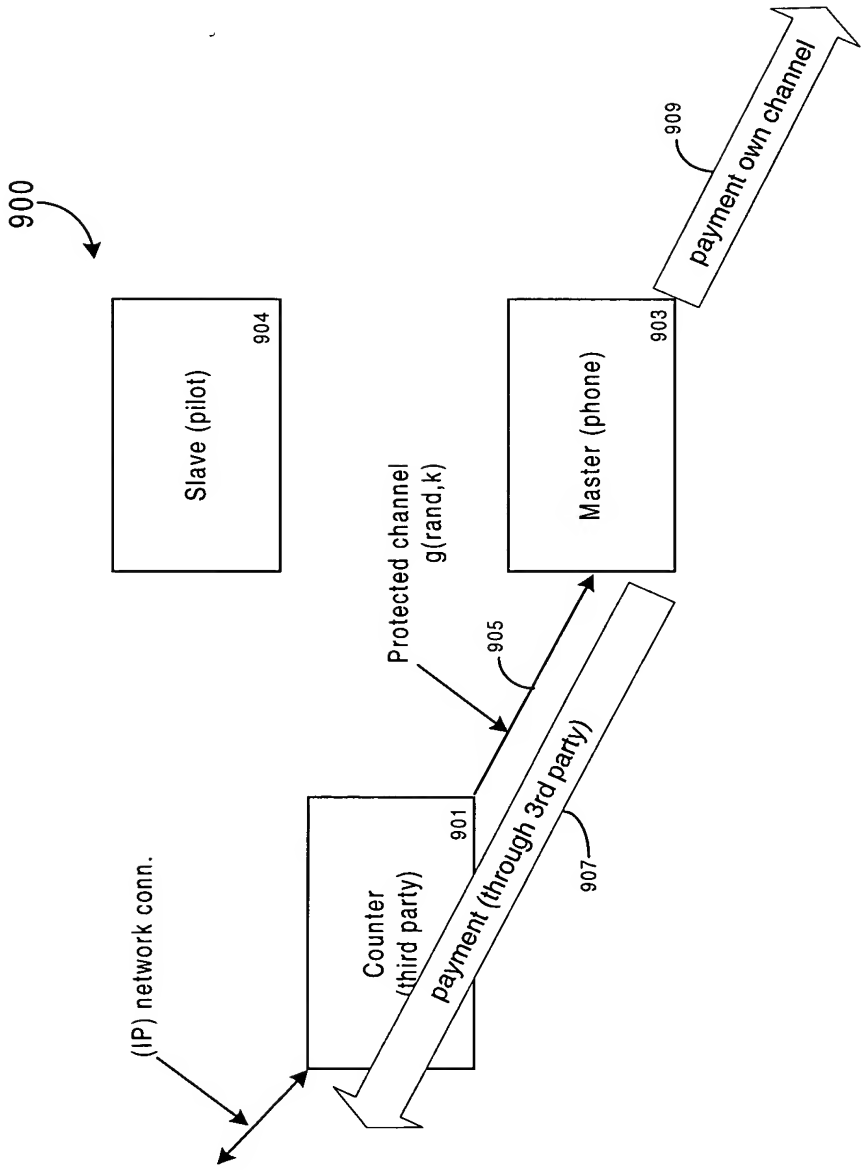

900
Slave (pilot)
904
Master (phone)
903
payment own channel
909
Protected channel
g(rand,k)
905
Counter
(third party)
901
Payment (through 3rd party)
907
(IP) network conn.

FIG. 8

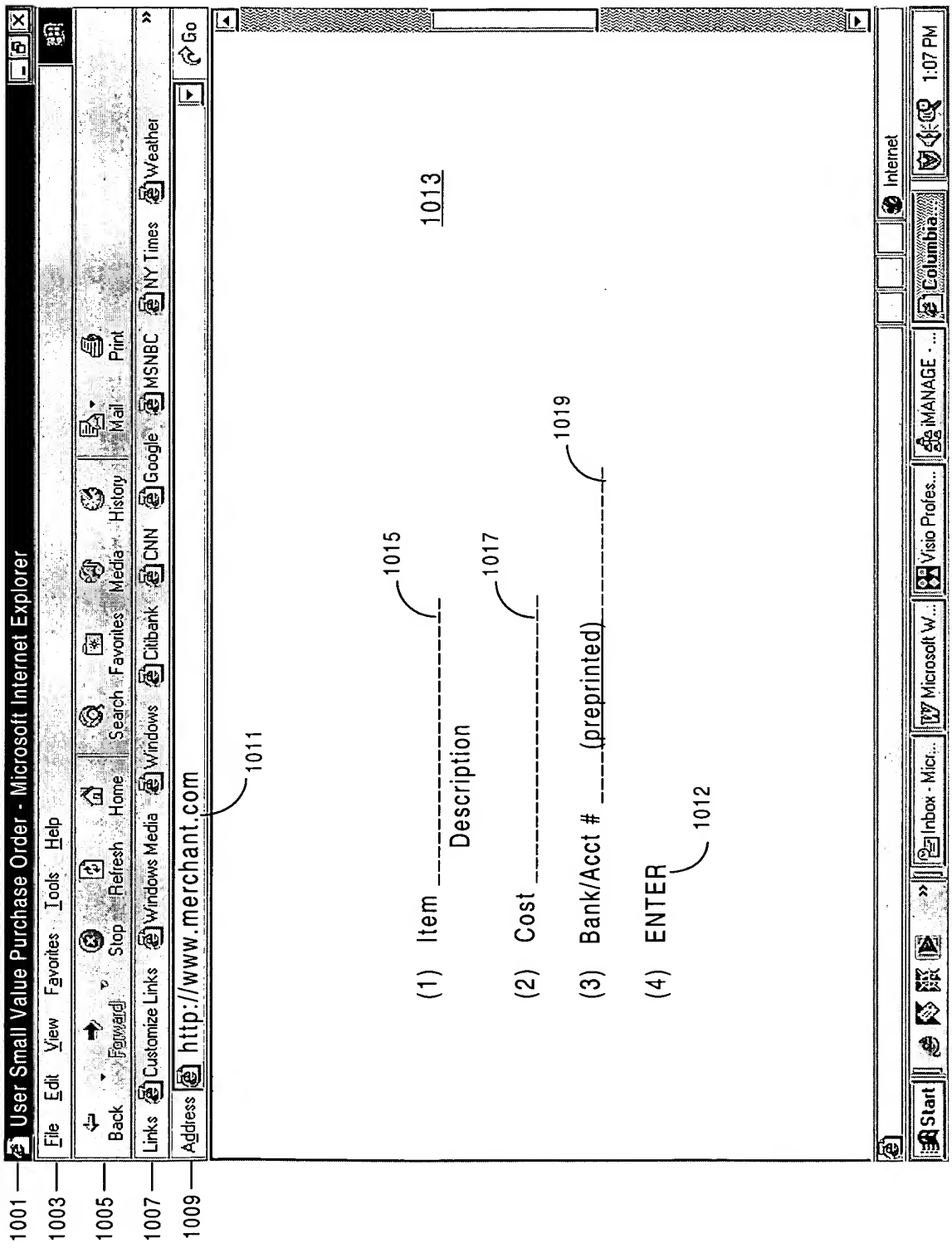

1001
1003
1005
1007
1009
User Small Value Purchase Order - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites Media History Mail Print
Links Customize Links Windows Media Windows Citibank CNN Google MSNBC NY Times Weather
Address http://www.merchant.com
Go
1011
1013
1015
(1) Item _____
Description
1017
(2) Cost _____
1019
(3) Bank/Acct # ____(preprinted)_____
(4) ENTER
1012
Start
Inbox - Micr...
Microsoft W...
Visio Profes...
MANAGE - ...
Columbia...
Internet
1:07 PM

Fig. 9

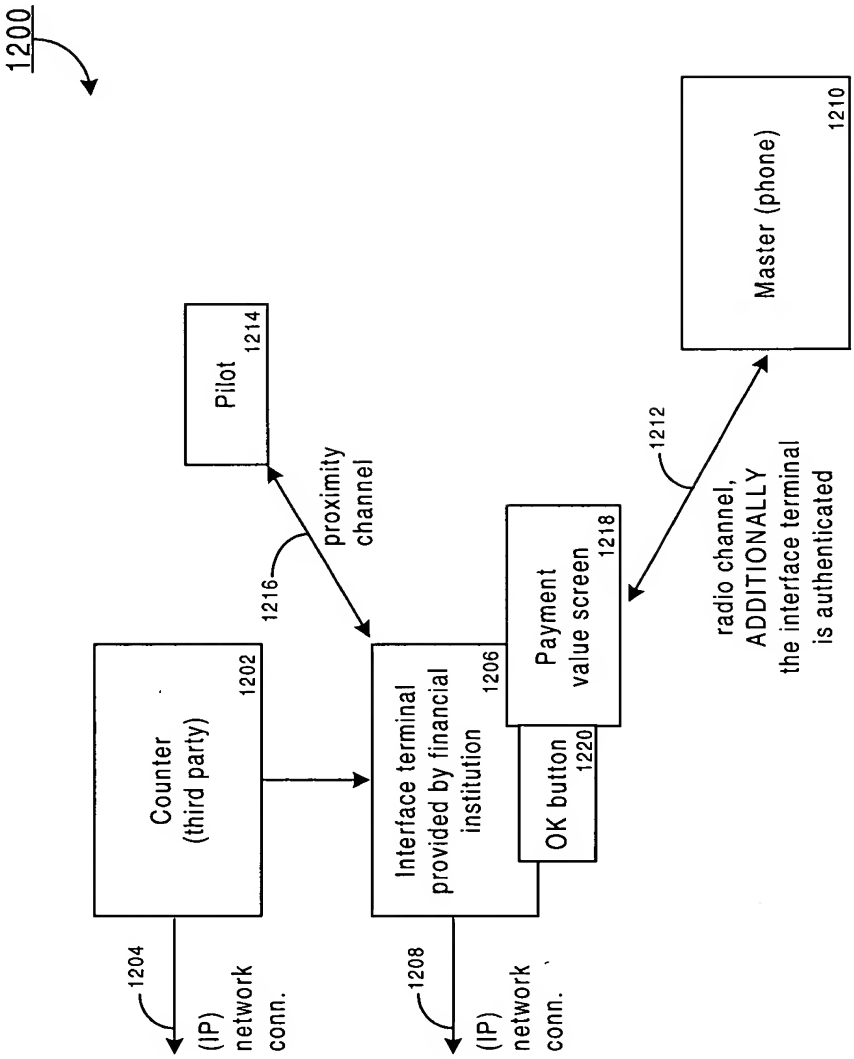

1200
Pilot
1214
proximity channel
1216
Master (phone)
1210
1212
radio channel, ADDITIONALLY the interface terminal is authenticated
Payment value screen
1218
Counter (third party)
1202
Interface terminal provided by financial institution
1206
OK button
1220
1204
(IP) network conn.
1208
(IP) network conn.

FIG. 10